

Auburn University at Montgomery

Policies and Procedures

Title: Software Acquisition Policy

Responsible Office: Information Technology Services (ITS)

I. PURPOSE

The purpose of this policy is to provide guidance to departments and employees regarding the acquisition of software for Auburn University at Montgomery (AUM).

II. POLICY

Software is an integral and necessary part to the operations of AUM. ITS has oversight over acquisition and maintenance of software. Review and approval of software or information technology services acquisition or renewals is required to ensure they meet or exceed regulatory statutes and best practices.

III. EFFECTIVE DATE

May 1, 2023

IV. APPLICABILITY

This policy applies to all departments, faculty, staff, and student workers, as well as contractors and vendors who are procuring software on behalf of the University. This policy applies regardless of the means of acquiring software such as purchasing card, requisition, or gift or the cost (including free software).

V. RESPONSIBILITY

ITS implements and administers the policy/procedure in detail.

Policy Responsible Office: Information Technology Services

Policy Responsible Executive: Chief Information Officer (CIO)

VI. DEFINITIONS

N/A

VII. PROCEDURES

General:

- ITS must be included in all software acquisitions to ensure compliance with the campus infrastructure.
- An approval process has been established that ensures review by appropriate offices, including the Center for Disability Services, ITS, and the Office of Financial and Administrative Services (Vetting Group).
- The Vetting Group must be contacted prior to the creation and dissemination of any requisition, bid, or request for proposal for software or information technology services.

- ITS will ensure that the software meets all operational requirements including server configurations, operating systems, and auxiliary or third-party software products (browser compliance etc.) as well as the user needs.
- In addition to the software, the Vetting Group will also review information technology services such as data hosting and/or storage services, whether data is hosted internally or by the vendor (or a cloud agent acting on behalf of the vendor).
- ITS will assess the level of internal support necessary for continuous operation, and the support services that are either provided by or will need to be purchased from the vendor.
- The software under review must provide a high-quality service that improves AUM's technology environment without jeopardizing network or server performance, data integrity or data security.
- Although a software or information technology-related service may have been through the review process, the software was approved for a specific scope of use. Further evaluation and approval may be required if the scope of use is changed or expanded, such as use by a different department or a use that expands the number of users.
- Departments or individuals seeking software or information technology services must contact ITS. A request must be made for any software or technology services acquisition, even if no ITS or university budget is requested or required.
- ITS will maintain a website listing approved software that has completed a recent vetting process.

Note: A software request for review does not alleviate requestors of following the regular procurement process. The requestor should start/continue the regular procurement (e.g. quote, PO, requisition, etc.).

Vendor Compliance:

- All vendors that provide cloud-based services must meet acceptable industry security standards and adhere to any additional AUM or Auburn University security procedures.
- Upon request, vendors must provide their SOC 1 or SOC 2 reports, or comparable compliance documents, and/or audit reports as needed that illustrate the vendor has committed an appropriate level of resources to data protection and security. Compliance documents may also include completed security specific questionnaires or contract amendments. The review will include, as applicable, compliance with AUM's technology accessibility standards, various other policy and compliance requirements (HIPAA, FERPA, etc.), and best practices to protect the confidentiality, integrity and availability of information through an appropriate information security controls review.
- All software that requires data exchange that may include sensitive or confidential information such as PCI, FERPA or HIPAA protected information must comply with all state and federal requirements.
- ITS must be included in vendor software demonstrations. ITS recommends comprehensive demonstrations prior to the purchase of any software, and will

work with vendors to arrange remote (video conference) demonstrations as needed.

- In cases where institutional data may be required for demonstration purposes, vendors must provide in advance all security compliance documentation as specified above, including written assurance that all data will be permanently removed from their systems following the demonstration.

VIII. SANCTIONS

Software and information technology services acquired without this review may be removed from AUM systems or access restricted.

IX. EXCLUSIONS

NONE

X. INTERPRETATION

The Chancellor has the authority to interpret this policy.

APPROVAL TO PROCEED:



DATE:

4/18/23

APPENDICES

NONE